WHITE & CASE LLP
Aaron Colodny (admitted *pro hac vice*)
555 South Flower Street, Suite 2700
Los Angeles, California 90071
Telephone: (213) 620-7700
Facsimile: (213) 452-2329
Email: aaron.colodny@whitecase.com

– and –

WHITE & CASE LLP

Gregory F. Pesce (admitted *pro hac vice*)
111 South Wacker Drive, Suite 5100
Chicago, Illinois 60606
Telephone: (312) 881-5400
Facsimile: (312) 881-5450
Email: jzakia@whitecase.com
        gregory.pesce@whitecase.com

WHITE & CASE LLP
Joshua D. Weedman
Samuel P. Hershey
Renza Demoulin
1221 Avenue of the Americas
New York, New York 10020
Telephone: (212) 819-8200
Facsimile: (212) 354-8113
Email: sam.hershey@whitecase.com

– and –

WHITE & CASE LLP
Keith H. Wofford
Southeast Financial Center
200 South Biscayne Blvd., Suite 4900
Miami, Florida 33131
Telephone: (305) 371-2700
Facsimile: (305) 358-5744
Email: kwofford@whitecase.com

Counsel to the Litigation Administrator

UNITED STATES BANKRUPTCY COURT
SOUTHERN DISTRICT OF NEW YORK

In re:	§ § §	Chapter 11
CELSIUS NETWORK LLC, *et al.*,	§ §	Case No. 22-10964 (MG)
Reorganized Debtors.[1]	§ § § § §	(Jointly Administered)

---

[1] The Debtors in these chapter 11 cases (the "**Chapter 11 Cases**"), along with the last four digits of each Debtor's federal tax identification number, are: Celsius Network LLC (2148); Celsius KeyFi LLC (4414); Celsius Lending LLC (8417); Celsius Mining LLC (1387); Celsius Network Inc. (1219); Celsius Network Limited (8554); Celsius Networks Lending LLC (3390); Celsius US Holding LLC (7956); GK8 Ltd (1209); GK8 UK Limited (0893); and GK8 USA LLC (9450). The location of Debtor Celsius Network LLC's principal place of business and the Debtors' service address in these chapter 11 cases is 50 Harrison Street, Suite 209F, Hoboken, New Jersey 07030.

MOHSIN Y. MEGHJI, LITIGATION ADMINISTRATOR, AS REPRESENTATIVE FOR THE POST-EFFECTIVE DATE DEBTORS,	§ § § § § § § § § § § § § § §	Adv. Proc. No. ____-_____
Plaintiff,		
v.		
CHRISTOPHER SPADAFORA and CLOUDFLARE, INC.,		
Defendant.		

COMPLAINT

Mohsin Meghji (the "**Plaintiff**" or the "**Litigation Administrator**"), in his capacity as Litigation Administrator of the estates of the above-captioned debtors and debtors-in-possession (collectively, the "**Debtors**," and together with their non-Debtor affiliates "**Celsius**" or the "**Company**") appointed pursuant to the *Modified Joint Chapter 11 Plan of Reorganization of Celsius Network LLC and its Debtor Affiliates* [Dkt. No. 4289] (the "**Plan**"), by and through his undersigned counsel, as Plaintiff in the above-captioned adversary proceeding, and based upon knowledge, information, belief, and the result of its investigation to date, alleges as follows:

NATURE OF THE ACTION

1.   While the world of cryptocurrencies may appear complex and novel, the legal claims at issue in this case are straightforward and old-fashioned. Defendants owed Celsius a duty to protect Celsius's assets under their control and to prevent obvious and known flaws in their systems from being exploited. They failed to do so, to the massive detriment of Celsius.

2.   Celsius was a global cryptocurrency platform and Bitcoin mining company that emerged from Chapter 11 bankruptcy on January 31, 2024.

3. Prior to Celsius's founding, holders of cryptocurrency had suffered from a lack of liquidity and of purchasing power because businesses refused cryptocurrency as a medium of exchange, and opportunities to earn returns on cryptocurrency assets were few and far between. Celsius was created to solve these problems, allowing users to transfer their cryptocurrency to Celsius in exchange for fiat or to earn rewards on those assets at favorable rates.

4. Celsius rapidly became one of the largest cryptocurrency finance platforms in the world, managing over $10 billion in customer assets.

5. As part of its multi-faceted investment strategies, Celsius deposited cryptocurrency with an organization called BadgerDAO, which offered another cryptocurrency platform for its members to use Bitcoin as collateral across decentralized finance platforms and to earn rewards.

6. One of the fundamental appeals of BadgerDAO's platform was its purported security. BadgerDAO's founder, Christopher Spadafora, repeatedly made bold claims about the security of his organization's platform, including to Celsius, which he told that he took "security VERY VERY seriously."

7. Despite this promise, Spadafora outsourced a significant portion of BadgerDAO's security to a third party called Cloudflare. Cloudflare is a leading, publicly-traded, connectivity cloud company that provides various web-based performance and security enhancement services.

8. Unfortunately for BadgerDAO, and ultimately Celsius, Cloudflare's services lacked reasonable safeguards, such as e-mail verification prior to account creation—safeguards that have been basic industry standards for years.

9. Predictably, Cloudflare's deficient security services led to a hacking incident, in which BadgerDAO was hacked and tens of millions of dollars' worth of Celsius's funds were stolen.

10.   The hack of BadgerDAO's systems, and the subsequent theft of tens of millions of dollars of Celsius's assets, were not caused by some unforeseen or complex attack on BadgerDAO's computer code, but rather by Cloudflare's failure to remedy an obvious and known issue that users had reported on public forums for several months before the hack.

11.   Indeed, users had warned Cloudflare that malicious actors were able to fraudulently register for Cloudflare accounts using only users' e-mail addresses. Users had also alerted Cloudflare that it should not be providing access to key passphrases before account verification was complete. Thus, Cloudflare was expressly put on notice of the significant weaknesses in its systems, but did nothing to remedy the problems until it was too late.

12.   Mr. Spadafora and his team at BadgerDAO also failed to implement basic security protocols that could have prevented the hack on BadgerDAO's end, such as rotating key passphrases—a common security practice that Mr. Spadafora implemented only after the hack.

13.   Unfortunately, Cloudflare's negligence in addressing this problem came back to haunt all those involved. In fact, by exploiting this exact vulnerability, a rogue hacker was able to access BadgerDAO's platform and steal Celsius's funds totaling more than $50 million. The hacker also drained other BadgerDAO users' accounts, for a total theft of $130 million.

14.   Just a few months later, on July 13, 2022, Celsius filed for Chapter 11 bankruptcy.

15.   Plaintiff brings this action to compensate the thousands of Celsius creditors who were harmed by Defendants' negligence.

THE PARTIES

16.   The Litigation Administrator brings this action pursuant to the Findings of Fact, Conclusions of Law, and Order Signed on November 9, 2023 Confirming the Modified Joint Chapter 11 Plan of Celsius Network LLC and its Debtor Affiliates (the "**Confirmation Order**")

4

[Docket No. 3972],[2] the Modified Joint Chapter 11 Plan of Reorganization of Celsius Network LLC and its Debtor Affiliates (Conformed for MiningCo Transaction) [Docket No. 4289] (the "**Plan**"), the Litigation Administrator Agreement [Docket No. 4297] (the "**Litigation Administrator Agreement**"), and section 1123 of the Bankruptcy Code. Pursuant to the Plan, Confirmation Order, and the Litigation Administrator Agreement, Plaintiff has the capacity, in his own right and name, to investigate, prosecute, compromise, and settle Recovery Causes of Action,[3] including this Action, on behalf of the Debtors and their Estates. The Debtors are: Celsius Network LLC; Celsius KeyFi LLC; Celsius Lending LLC; Celsius Mining LLC; Celsius Network, Inc.; Celsius Network Limited; Celsius Networks Lending LLC; Celsius US Holding LLC; GK8 Ltd; GK8 UK Limited; and GK8 USA LLC.

17.   Defendant Cloudflare, Inc. is a publicly-traded corporation with its principal place of business at 101 Townsend Street, San Francisco, California 94107.

18.   Defendant Christopher Spadafora is the founder and Senior Community Manager of BadgerDAO, as well as a member. Upon information and belief, Mr. Spadafora is a resident of Toronto, Canada. In performance of his activities for BadgerDAO, Mr. Spadafora actively engaged in business in or directed at the United States.

JURISDICTION AND VENUE

19.   The United States Bankruptcy Court for the Southern District of New York (the "**Bankruptcy Court**" or the "**Court**") has jurisdiction over this Adversary Proceeding pursuant to 28 U.S.C. §§ 157 and 1334 and the Amended Standing Order of Reference, No. M-431, of the

---

[2]   "Docket No." refers to the docket of *In re Celsius Network LLC, et al.*, Case No. 22-10964 (MG) (Bankr. S.D.N.Y. July 13, 2022). Documents filed on this docket can be accessed free of charge at https://cases.stretto.com/celsius/ (the "**Claims Agent Website**").

[3]   Capitalized terms used but not otherwise defined herein shall have the meanings ascribed to them in the Plan, Confirmation Order, and/or Litigation Trust Agreement.

United States District Court for the Southern District of New York, dated January 31, 2012.

20.   The Adversary Proceeding is a core proceeding pursuant to 28 U.S.C. § 157. This Court has jurisdiction to hear and to determine this proceeding and to enter a final order and judgment. In the event that this Court or any other court finds any part of the Adversary Proceeding to be "non-core," this Court has non-core concurrent jurisdiction over this proceeding under 28 U.S.C. § 1334 because the relief sought herein relates to the Chapter 11 Cases and will have a material impact on the administration of Debtors' Estates.

21.   Plaintiff consents to entry of final orders and judgments by this Court in this Adversary Proceeding pursuant to Bankruptcy Rule 7008. Plaintiff also consents to entry of final orders or judgments by this Court if it is determined that this Court, absent consent of the parties, cannot enter final orders or judgments consistent with Article III of the United States Constitution.

22.   This Court has personal jurisdiction over Defendants because, as described above, Defendant Cloudflare resides and is located in the United States, and Defendant Spadafora has actively engaged in business in or directed at the United States. Personal jurisdiction is thus sufficient pursuant to Bankruptcy Rule 7004(d) and (f).

23.   This Court has jurisdiction over Defendants inasmuch as Defendants have maintained minimum contacts with the United States in connection with the claims asserted in this Complaint. This Court also has jurisdiction over Defendants pursuant to Bankruptcy Rules 7004(d) and (f) and New York Civil Practice Law & Rules § 302 (McKinney 2008) because Defendants purposefully availed themselves of the laws of the United States and the State of New York by, among other things, doing or transacting business in the United States and in the State of New York, which gives rise and/or relates to the claims at issue in this Adversary Proceeding.

24.   Venue is proper pursuant to 28 U.S.C. §§ 1408 and 1409 because this Adversary

Proceeding arises under and is related to the Debtors' bankruptcy case pending in this Court.

FACTUAL BACKGROUND

A.   Celsius

25.   Celsius was founded in 2017. Celsius planned to offer two primary products. First, customers could transfer their cryptocurrency assets to Celsius and take out loans in fiat collateralized against these assets. Second, and of relevance for this complaint, customers could transfer their cryptocurrency assets to Celsius in exchange for weekly interest. Celsius planned to lend those cryptocurrency assets to hedge funds, family offices, and crypto funds to generate yield. In short, customers would deposit digital assets onto the Celsius platform, and Celsius would lend the coins to third parties to earn yield.

26.   Celsius rapidly became one of the largest cryptocurrency finance platforms in the world and provided financial services to institutional, corporate, and retail clients across more than 100 countries. By July 2022, Celsius had approximately $1.7 million registered users and managed approximately $6 billion in assets.

27.   Unfortunately, Celsius's initial successes would not last.

28.   In the spring of 2022, what is now referred to as a "crypto winter" set on the cryptocurrency space. On May 7, 2022, a spike in migration of assets off the Celsius platform turned into an explosion. The cryptocurrency token, TerraUSD ("**UST**"), suffered a significant loss of value that sent shockwaves through the entire cryptocurrency market (the **"Terra Luna Collapse"**). Celsius had approximately $940 million deployed on the Terra blockchain and had lent $41 million to Three Arrows Capital, which entered liquidation as a result of the Terra Luna Collapse. In the face of the Terra Luna Collapse, rumors swirled around Celsius and its stability.

Customers withdrew billions of dollars' worth of cryptocurrency assets from the Celsius platform in the second week of May 2022.

29.   Celsius faced an internal liquidity crisis. It had billions of dollars invested in illiquid investments but insufficient assets to address customer withdrawal requests. Celsius also had more than one billion dollars in loans collateralized by cryptocurrency that was dramatically decreasing in value. It required additional collateral to survive margin calls. By May 16, 2022, Celsius's liquidity had dropped by 40% due to customer withdrawals and steep price declines in BTC and ETH.

30.   On June 12, 2022, in response to customer withdrawal demands and increasing volatility in the cryptocurrency markets, Celsius paused all withdrawals from its platform to prevent further erosion of value. Hundreds of thousands of customers who still had assets on the platform were left without recourse, unable to withdraw or sell their coins.

B.   The Chapter 11 Cases

31.   On the Petition Date, the Debtors, other than GK8 Ltd, GK8 UK Limited, and GK8 USA LLC (collectively, the "**GK8 Debtors**"), filed voluntary petitions for relief in this Court under chapter 11 of the Bankruptcy Code. On December 7, 2022, the GK8 Debtors also filed voluntary petitions in this Court under chapter 11 of the Bankruptcy Code. All of these Chapter 11 Cases were consolidated for procedural purposes only and are jointly administered pursuant to Bankruptcy Rule 1015(b).[4]

---

[4]   *See Order Directing (I) Joint Administration of the Chapter 11 Cases and (II) Granting Related Relief* [Docket No. 53]; *Order Directing (I) Joint Administration of the Chapter 11 Cases and (II) Granting Related Relief* [Docket No. 1648].

32.   On November 9, 2023, the Court entered the Confirmation Order, pursuant to which the Bankruptcy Court approved and confirmed the Plan for all of the Debtors (as amended, supplemented, or modified from time to time).

33.   On January 31, 2024, the Plan became effective.[5] As part of the Plan, the Litigation Administrator was appointed to prosecute, settle, or otherwise resolve any claims belonging to the Estates and to serve as the Estates' representative in certain litigation, including causes of action under chapter 5 of the Bankruptcy Code.[6] The Litigation Administrator is charged with maximizing distributions to the stakeholders, including victims of Celsius's collapse.

C.   **BadgerDAO**

34.   BadgerDAO is a Decentralized Autonomous Organization ("**DAO**") founded by Defendant Spadafora. Its stated mission is to allow its members to use Bitcoin as collateral across decentralized finance ("**DeFi**") applications.[7]

35.   Like most DAOs, BadgerDAO provides for a bottom-up governance system, whereby members in possession of governance tokens can vote on initiatives via the blockchain. If approved, those initiatives are implemented via smart-contracts, which are logically-coded agreements that dictate decision-making based on underlying activity on a blockchain.

36.   Although DAO members vote on large-scale initiatives, they cannot manage the DAO's everyday operations via blockchain voting. Instead, the most involved community members like Defendant Spadafora are required to handle the DAO's daily administration, including platform development, the negotiation and signature of contracts with service providers, and communication with users.

---

[5]   *See Notice of Occurrence of Effective Date of Debtors' Modified Chapter 11 Plan of Reorganization and Commencement of Distributions* [Docket No. 4298].

[6]   *See* Plan, Art. IV.L.

[7]   DeFi applications provide an interface that automates transactions between users.

37.   In a January 2, 2024 interview, Mr. Spadafora explained that "there's a whole ecosystem around BadgerDao that believes in its potential . . . there is [*sic*] the councils that make decisions around treasury, that make decisions around operations, and then there is this whole group of contractors that brings this software to life." Mr. Spadafora added that as a result "[t]here is this asymmetry of information between a random person and a person that's actually writing the code or working with the security service provider."

38.   Mr. Spadafora regularly communicated with BadgerDAO's users via his dedicated @badger e-mail account, from BadgerDAO's X (formerly Twitter) account, and from his own dedicated account, "Spadaboom1." Mr. Spadafora, who appeared on several live broadcasts and podcasts to promote BadgerDAO and answer user questions regarding BadgerDAO, was described in the press as the "operations lead" and served as BadgerDAO's "Senior Community Manager," which, according to press reports, included building and managing relationships with the Badger community, providing support and guidance to the community, and promoting engagement and excitement around Badger and the DeFi ecosystem.

39.   BadgerDAO offers several products to its users. These include Sett Vaults, a product that allows users to deposit and earn yield on their synthetic bitcoin assets, and BADGER, an Ethereum-based[8] token used for governance purposes and distribution of rewards to BadgerDAO users.

40.   Customers interact with BadgerDAO products, invest their cryptocurrencies, and approve transactions via the Badger app, which is designed and maintained by Badger developers. To edit the user interface or functions available to customers, Badger developers access the developer-end of the Badger app, called the Application Programming Interface or "**API**," and

---

[8]   Ethereum is a decentralized blockchain platform. Smart contracts allow participants to transact with each other without a trusted central authority.

implement computer code therein. Access to the BadgerDAO API allows a developer to perform

actions such as changing the user interface of the BadgerDAO app (*i.e.*, the way the app looks and

is organized), changing the type of transactions available to customers, or even changing the type

of underlying transaction performed in response to a customer's prompt.

41.   Upon information and belief, BadgerDAO contracted with Cloudflare to secure

access to its API. Developers could only access the BadgerDAO API with an "API key"—a

passphrase that Cloudflare would issue for BadgerDAO developers. To view the Cloudflare-

generated API keys, BadgerDAO developers needed to log into their Cloudflare account.

42.   A new joiner to BadgerDAO's developer team thus would have needed to register

for a Cloudflare account, using their BadgerDAO-issued e-mail address. Upon receiving a

registration request, Cloudflare would automatically generate a unique e-mail verification link and

send it to the e-mail address used to register. The BadgerDAO developer then needed to log into

their BadgerDAO e-mail account, open Cloudflare's automatically-generated e-mail, and click on

the verification link. The act of clicking the verification link activated the Cloudflare account and

the API keys contained therein.

43.   By following these steps, the developers confirmed to Cloudflare that they had

access to the e-mail address they used to register for a Cloudflare account, and that the account

creation request was made by an authorized BadgerDAO user.

44.   The use of an e-mail verification link to complete account registration for any

service has long been an industry standard. It serves as a validation mechanism to confirm that

the provided email address belongs to the user and is legitimate. By clicking on the link, the user

signifies that they have access to the email account associated with the email address provided to

register for the account, which in turn prevents unauthorized access.

D.   Celsius Invests in BadgerDAO

45.   In early 2021, as part of its multi-faceted investment strategy discussed above (*supra* ¶¶ 25-26), Celsius began to invest its customers' cryptocurrency deposits through external platforms like—and including—BadgerDAO's DeFi platform.

46.   On January 16, 2021, Celsius Chief Executive Officer Alexander Mashinsky received an e-mail from fellow cryptocurrency enthusiast Arben Kane, introducing him to Mr. Spadafora and BadgerDAO. Upon information and belief, Mr. Mashinsky subsequently met with Mr. Spadafora, who persuaded Celsius to invest its customers' assets on BadgerDAO's platform.

47.   At multiple points in 2021, Celsius employees had conversations with Mr. Spadafora concerning BadgerDAO's infrastructure, protocols, and products. These conversations took place via e-mail, Telegram, Slack, and over the phone.

48.   Over the months these conversations took place, Mr. Spadafora established a relationship of trust with Celsius employes, providing updates regarding the advancement of certain BadgerDAO projects, advertising the launch of new BadgerDAO products, providing investment advice to Celsius, and even providing directives to Celsius for how it should organize its assets so it could cast votes in favor of certain community initiatives on BadgerDAO. For example:

- In a July 9, 2021 Slack chatroom with numerous Celsius employees, Mr. Spadafora stated that "[w]e recently launched our new Curve BTC vaults . . . [w]ith a decent Badger boost these vaults have 3-4x better APYs then [sic] going to Convex direct."

- On July 12, 2021, Mr. Spadafora told the same group of Celsius employees: "[i]f you have any questions around how it works, how to maximize returns please let me know. Looks like some of your deployment wallets are already on Curve LPing BTC. So would really help juice up returns to put those in Badger."

- On October 29, 2021, Mr. Spadafora advised a group of Celsius employees that: "I'd suggest withdrawing your CVX from there, either depositing that into the new bvccvx/cvx CURVE pool and/or locking a % of them in our vault (earning 20%) and then LPing that with CVX on Curve. Then taking that and depositing in the new vault."

- On October 12, 2021, Mr. Spadafora wrote to the same group of Celsius employees about a "couple of things [that] are top of mind that I figured you'd want to take advantage of in the Badger ecosystem," stating that "[w]e suggest claiming your bvx through the claim button top right of the app. Withdrawing CVX from that vault and depositing it in Vote Locked CVC vault."

- On the same day, Mr. Spadafora advised Celsius on how to vote on one of the community initiatives, stating that "Badger is the only designated group voting to increase APY on Curve BTC pools. . . . If you have BTC in Curve regardless if its [sic] in Badger or not you are going to want Badger to vote to ensure those pools get higher CRV rewards. Also we are spending quite a bit of $$ on bribing other CVX holders via Votium app to vote on BTC pools. Many of those bribes will go back to those in the Vote Locked Convex vault. The next vote starts tomorrow. If you can withdraw CVX and deposit in voted locked CVX it will be eligible to vote for the Curve rewards starting Thursday."

- Hopeful that Celsius would follow his recommendation, Mr. Spadaora wrote again to the same group of Celsius employees the next day: "we are the only ones voting to increase CRV rewards on BTC pools. Lock CVX with Badger to increase your yield on BTC deposits even if they aren't in Badger. Locked CVX in Badger will have a Curve liquidity pool for easy exit so you don't have to wait the 16 weeks. Next vote is in 9 hours so if you can lock before then we can boost yield for BTC for the next 2 weeks before the next vote."

49.   Celsius employees therefore understood Mr. Spadafora to be the mouthpiece for the team of developers and community members managing BadgerDAO's products, as evidenced by several Celsius employees reaching out to Mr. Spadafora's Slack handle with questions addressed to "Badger team."

50.   During 2021, Celsius Chief Security Officer Shiran Kleiderman had conversations with Mr. Spadafora and other individuals holding themselves out to represent BadgerDAO concerning BadgerDAO's security protocols and infrastructure. During these interactions and on

several other occasions, Mr. Spadafora communicated to Celsius that BadgerDAO's security protocols were robust.

51.   On May 14, 2021, Mr. Spadafora e-mailed Celsius to summarize key points about security, stating that "[a]t Badger we take security VERY VERY seriously," and that "we worked with Fireblocks to have our app be fully integrated into their system so their customers[, including Celsius,] can maintain their security standard while depositing in Badger." Mr. Spadafora also sent Celsius an article, which stated that the partnership between Fireblocks and BadgerDao would allow Fireblocks' institutional clients, like Celsius, to "securely hold Badger assets on their platform and put their Bitcoin to work through the Badger protocol."

52.   In reliance on Mr. Spadafora's assurances, in February and March 2021, Celsius began purchasing BADGER tokens for the equivalent of $3.5M USD and staked those tokens in the BADGER vault.

53.   Over the course of the next several months, Celsius continued to invest Celsius assets on the BadgerDAO platform, eventually placing hundreds of Bitcoins in BadgerDAO's Sett Vaults through a MetaMask wallet to earn yield on the invested assets.

E.   BadgerDAO's Poorly Protected Platform Is Hacked

54.   On December 2, 2021, a phishing incident occurred on BadgerDAO's platform.[9]

55.   According to post-mortem reports of the attacks, a hacker used a compromised API key created without the knowledge or authorization of Badger engineers to inject malicious code in the Badger API. The malicious code prompted users to authorize hidden transactions, and eventually allowed the hacker to transfer the compromised users' funds to their own account.

---

[9]   The closing price of bitcoin on December 2, 2021 was approximately $56,516.20.

14

56.   Ultimately, the hacker made off with approximately $130 million in user funds, including approximately 900 Bitcoin that Celsius had deposited on the platform with a value of more than $50 million.

57.   After the incident, BadgerDAO hired cybersecurity firm Mandiant and blockchain-analysis firm Chainalysis to investigate the hack.

58.   Mr. Spadafora informed Celsius Chief Security Officer Shiran Kleiderman on December 15, 2021 that "[w]e've worked with Mandient [*sic*] to review our changes to the front end to ensure we aren't in a comprised [*sic*] state and have initiated a full audit and rearchitecture with Halborn that sould be completed in 4 weeks. All contract were upgraded to blacklist exploiter addresses from interacting with Badger."

59.   In an August 2022 blog post, which has since been deleted, BadgerDAO and Mandiant released a statement detailing how the hack took place.

60.   The blog post stated that in late September 2021, users on a Cloudflare community support forum had reported that unauthorized users were able to create accounts and create or view API keys before email verification was completed. It was noted that an attacker could use a legitimate e-mail address to register for a Cloudflare account, immediately obtain the ability to view the API key, then wait for the email to be verified and for the account creation to be completed, which would in turn activate the API key, and they would then have access to the user's API.

61.   The users who reported this vulnerability in Cloudflare's system were not related to Celsius or to BadgerDAO, but they had experienced the same issue that would ultimately lead to the hack of BadgerDAO's platform.

62.   One user wrote on September 27, 2021: "there is a huge difference between someone creating an account on accident [with an] incorrect email address [as opposed to] when someone can use your email address to register and apparently login to create API token. That's not a mistake, that's an [*sic*] hack attempt." That same user continued: "[s]o Cloudflare can and really should do something about this. Email validation should be mandatory before an account gets created at all."

63.   A different user with the username "dave73" responded on September 27, 2021: "I am here because two people in our company have received this [fraudulent verification] email, me being one of them. I think the angle the attackers are going for here is to create the account and add the API keys, and then wait and hope that the email owner clicks that verification link. If they do, then those API keys can be used to make API calls and carry out malicious activity. . . . CloudFlare, FIX THIS NOW. This is a bug in your system. The account should not be active until the user is verified. This is a serious security issue that is obviously a viable attack metric as it is being used more and more by attackers. FIX THIS NOW."

64.   On September 29, 2021, username dave73 wrote again on the forum to inform fellow users that a ticket logged with Cloudflare had received the following response: "Our engineering team has confirmed that they will make changes to the sign up process based on the recent increase of unrecognized sign up reports." Upon information and belief, Cloudflare never contacted its users to warn them that their accounts may have already been compromised.

65.   Upon reviewing Cloudflare logs after the exploit, BadgerDAO identified unauthorized account creation and API key generation for three BadgerDAO accounts; two in late August, one in early September. In mid-September, BadgerDAO unknowingly completed the

account creation for one of these three compromised accounts, which were used for legitimate BadgerDAO management activities.

66.   On November 10, 2021, the attacker began using their access to BadgerDAO's API to insert malicious code into BadgerDAO's app.

67.   Whenever a user initiated a transaction through the BadgerDAO app, the hacker's code would intercept the intended transaction and insert an underlying request to transfer all of the victim's tokens to the attacker's address. The user thought they were approving their intended transaction, but they were in fact authorizing the hacker's underlying request. A first malicious approval was made on November 20, 2021. The hacker accumulated rogue approvals, waiting for a user with a significant amount of funds in their account to provide a rogue approval. This happened 11 days later.

68.   On December 1, 2021, a user related to Celsius, which held more than $50 million worth of tokens in its account, approved a rogue request. The attackers quickly responded by withdrawing all of these funds and also draining all other accounts for which they had received approvals until then, for an approximately $130 million theft.

69.   After the exploit, recognizing that its security measures had been inadequate, BadgerDAO took efforts at remediation and initiated new protocols, including multifactor authentication, password changes, and the regular rotation of Cloudflare API keys. Upon information and belief, these measures were taken by Mr. Spadafora and his team.

F.   Recovery and Restitution

70.   In the aftermath of the hack, BadgerDAO attempted to recover some of the stolen funds and to provide restitution to injured users. The restitution was split into three tranches.

71.   The first tranche involved "reclaimable" assets. After the attack, the hacker's address had $9.2 million in vault tokens that BadgerDAO could seize in a one-time operation. Once recovered, these funds were distributed to users. 37% of affected users received a token-for-token refund on losses through this process.

72.   The second tranche involved stolen BADGER tokens, worth approximately $2.8 million. BadgerDAO used some of the outstanding BADGER supply not earmarked for other purposes to restore those stolen tokens. The assets of 17% of those affected by the attack were restored through this process.

73.   The third tranche concerned the vast majority of the funds, totaling $121 million, which were not recoverable and could not be replaced. To compensate these victims for their losses, the BadgerDAO community voted to create a remedial token known as a remBadger token. Two million in BADGER tokens were allocated towards progressive restitution via the remedial token over the course of two years, and the amount that victims would receive at the end of the two-year period would depend upon the evolution in the price of the BADGER token.

74.   As part of the remediation efforts, Celsius recovered 89.89 bitcoin as restitution on January 13, 2022, and $2.1 million in remedial tokens on March 17, 2022. The closing price of bitcoin on January 13, 2022 was approximately $42,602.76, meaning the 89.89 bitcoin were worth approximately $3,829,562.10.

75.   Celsius, which suffered over 40% of the total losses from the hacking incident, was also allocated 901 remBadger. However, on March 18, 2022, a Celsius employee accidentally withdrew the remBadger tokens, which, at the time of withdrawal were worth approximately $2.1 million. Unbeknownst to the employee, withdrawing the remBadger tokens forfeited Celsius'

18

entitlement to any additional recoveries. Forfeited future restitution rewards were then distributed among remaining remBadger holders.

76. Once Celsius realized what had happened, it notified the Badger team, but the Badger community refused to allow Celsius to redeposit its remBadger and recover any future amounts.

77. While Celsius never should have suffered a loss in the first place and never should have been in a position to accept remBadger in place of its bitcoin (a trade it did not agree to before it deposited bitcoin the BadgerDAO platform), the terms of the remBadger restitution program would have left Celsius with massive losses even in the best-case scenarios.

78. BADGER, which had been trading at around $25 since its inception, would have needed to reach $60 for Celsius and other victims to make a full recovery. As of the date of this filing, BADGER trades at around $3.

79. Despite this effort at restitution, Celsius still suffered massive losses as a result of the hacking incident.

FIRST CAUSE OF ACTION

Common Law Negligence – Defendant Cloudflare, Inc.

80. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

81. Cloudflare owed BadgerDAO and all its governing members, including Celsius, a duty to implement adequate security protocols for the issuance of API keys granting access to BadgerDAO's API.

82. By agreeing to secure access to BadgerDAO's accounts containing sensitive passphrases like API keys, Cloudflare took on a duty to act as a reasonably prudent person would in that situation.

83.   The prevalent industry standard for all confidential account information that is secured behind a password-locked screen is that it must remain confidential until a request for access has been authenticated. That is the standard that Celsius, as both a member and customer of BadgerDAO, reasonably expected when it relied on Cloudflare's systems to secure its investments on BadgerDAO's platforms.

84.   To the extent that a flaw in Cloudflare's system initially went unnoticed but was eventually fixed, it was foreseeable that malicious actors may have gained access to Cloudflare's clients' sensitive information before the bug was remedied. All BadgerDAO members, including Celsius, reasonably expected that Cloudflare would warn its users if a bug may have compromised their sensitive information prior to being remedied. Yet Cloudflare failed to warn users of the vulnerability.

85.   By issuing API keys prior to account verification and not warning users of the vulnerability once it was discovered, Cloudflare breached its duty to BadgerDAO, and consequently, its duty to Celsius.

86.   Cloudflare's breach allowed the hacker to remain undetected for over two months, as the hacker first obtained an API key in mid-September and only deployed their first fraudulent request for transfer of funds on November 20, 2021. Therefore, Cloudflare's breach was the proximate and but-for cause of Celsius's injury.

87.   Cloudflare's failure to exercise the degree of care for the safety of others, which the industry standard requires and which a person of ordinary prudence would exercise under similar circumstances, constitutes negligence.

88.   Cloudflare's negligence caused Celsius to lose more than $50 million in assets stored on the BadgerDAO platform.

SECOND CAUSE OF ACTION

Common Law Gross Negligence – Defendant Cloudflare, Inc.

89.   Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

90.   Cloudflare owed BadgerDAO and all its governing members, including Celsius, a duty to implement adequate security protocols for the issuance of API keys granting access to BadgerDAO's API.

91.   By agreeing to secure access to BadgerDAO's accounts containing sensitive passphrases like API keys, Cloudflare took on a duty to act as a reasonably prudent person would in that situation.

92.   Cloudflare breached its duty to Celsius when it failed to remedy the known vulnerability in its systems described in paragraphs 56-60 *supra*, which created an unreasonable risk of harm to all users of BadgerDAO, including Celsius. Cloudflare was made aware of the vulnerability and knew it meant that a malicious actor could access the developer-end or API of its clients' platforms. Cloudflare also knew that many of its clients' APIs were designed to secure funds. This was the case for BadgerDAO, which held millions of dollars in customer funds. By failing to immediately remedy the vulnerability, and by subsequently failing to notify users that their APIs, and therefore their funds, might have been compromised, Cloudflare created an unreasonable risk of harm to its users, including BadgerDAO, and in turn, to BadgerDAO's users, including Celsius.

93.   Cloudflare's failure to act was therefore grossly negligent.

94.   As a result of Cloudflare's breach, and because of Cloudflare's failure to exercise even slight care or diligence in fixing or notifying BadgerDAO of a known issue that had been

reported on multiple occasions, Celsius has suffered damages, losing more than $50 million in assets as a result of the hack of BadgerDAO's platform.

<div align="center">**THIRD CAUSE OF ACTION**</div>

<div align="center">**Common Law Breach of Fiduciary Duty – Defendant Christopher Spadafora**</div>

95.   Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

96.   Defendant Spadafora owed a duty to Celsius arising from the relationship he established with Celsius and its officers. Mr. Spadafora held himself out as the representative of BadgerDAO, e-mailing and messaging Celsius directors and officers and attending conference calls with Celsius directors and officers on behalf of BadgerDAO. *See supra* ¶¶ 45-53. On multiple occasions, including in an e-mail dated May 14, 2021, Mr. Spadafora reassured Celsius officers concerning the security of BadgerDAO's systems. *See supra* ¶¶ 46-53. Based on Mr. Spadafora's statements and representations, Celsius placed trust and confidence in Mr. Spadafora's management of the DAO he had founded.

97.   Defendant Spadafora was in a dominant and superior position to Celsius when it came to understanding BadgerDAO and its security protocols, as well as capacity to manage BadgerDAO's day-to-day administration, engagements with service providers, platform development, or internal security audits. As the founder and general manager of BadgerDAO, Mr. Spadafora handled decision-making that voting members were unable to vote on. As such, Celsius was forced to place its trust in Mr. Spadafora's and let Mr. Spadafora handle day-to-day management of BadgerDAO.

98.   For these reasons, Mr. Spadafora was under a duty to act for the benefit of Celsius and other users on matters related to BadgerDAO, including BadgerDAO service providers, and BadgerDAO protocols. The duty that Defendant Spadafora owed to Celsius required him to act

for Celsius's benefit on matters related to Celsius's investments into BadgerDAO, including the security of Celsius's funds on the BadgerDAO platform. Mr. Spadafora owed Celsius a duty to *inter alia* put in place procedures such that an attack on a single developer's account would not result in a multi-million dollar theft.

99.   Defendant Spadafora breached that duty by failing to implement reasonably expected safeguards that have been industry standards for years, including, but not limited to, rotating API keys. Defendant Spadafora also breached that duty when he decided to use Cloudflare's free services, irrespective of the standard of care that Cloudflare may exercise when securing non-paying clients' apps, and despite the fact that BadgerDAO held millions of dollars in user assets.

100.   Defendant Spadafora' breach of his duties allowed the hack, which caused Celsius to lose more than $50 million in assets.

REQUESTED RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter a judgment in favor of plaintiff awarding:

i.   Compensatory damages to Plaintiffs in an amount to be determined at trial;

ii.   Punitive damages in an amount to be determined at trial;

iii.   Allowable costs and attorneys' fees pursuant to Federal Rule of Civil Procedure 54, or any other applicable provision or principle of law;

iv.   Prejudgment interest; and

v.   Any other relief which the court may deem just and proper.

DATED: July 12, 2024

                /s/ *Joshua D. Weedman*
               WHITE & CASE LLP
               Joshua D. Weedman
               Samuel P. Hershey
               Renza Demoulin
               WHITE & CASE LLP
               1221 Avenue of the Americas
               New York, NY 10020
               Telephone: (212) 819-8200
               jweedman@whitecase.com
               sam.hershey@whitecase.com
               renza.demoulin@whitecase.com